Title	Data Protection Policy
Document Type	Policy
Reference	GOVERNANCE
Policy Owner	Data Protection Officer
Approved By	Finance and General Purpose Committee
Approval Date	July 2026
Review Date	July 2028
Publication Status	External/Internal/Confidential

Please contact The College if you require a copy of this Policy in an alternative format.

CONTENTS

York College - Data Protection Policy 3
1.0 Introduction 3
2.0 Status of the Policy 3
3.0 Related Policies & Procedures 3
4.0 Definitions 4
5.0 Roles, Responsibilities & Accountability 5
5.1 College Governors 5
5.2 Information Asset Owners 5
5.3 Data Protection Officer (DPO) 5
5.4 Staff (including consultants and contractors) 6
5.5 Students 6
6.0 The Data Protection Principles 6
7.0 Lawful Basis For processing (Data Asset Register) 7
8.0 Transparency and Privacy Notices 7
9.0 Data Security 8
10.0 Information Security Breaches 8
11.0 Record of Processing Activities (Asset Register) 9
12.0 Processing Special Category Data 10
13.0 Individual's Rights and Subject Access Requests 10
14.0 Subject Consent 11
15.0 Information Sharing 11
16.0 Direct Marketing 13
17.0 International transfers 13
18.0 Publication of College Information 13
19.0 Retention of Data 14
20.0 Privacy by design 14
21.0 Data protection impact assessments (DPIAs) 14
22.0 Complaints 15
23.0 Registration 15
24.0 Key Contacts 15

York College- Data Protection Policy

1.0 Introduction

The College needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles which are set out in the General Data Protection Regulations (GDPR).

The College is committed to complying with the General Data Protection Regulation (GDPR) and any legislation enacted in the UK in respect of the protection of personal data (together "data protection legislation"). This policy sets out how the College manages those responsibilities.

The College maintains a safe and secure environment for everyone. As part of this commitment, the college upgrades its CCTV coverage across campus to reduce the risk of vandalism and strengthen overall safety and security for students, staff and visitors. CCTV helps the College to respond more effectively to incidents and ensures our community remains a safe place to learn and work.

2.0 Status of the Policy

The Data Protection Policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failure to follow the policy may therefore result in disciplinary proceedings.

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the designated data controller initially. If the matter is not resolved, it should be raised as a formal grievance.

Staff will receive information relating to this policy and its operation as part of their induction to the College.

3.0 Related Policies & Procedures

IT & Data Security Policy
Data Breach Policy
Data Retention and Deletion Policy
Subject Access Procedure
Complaints & compliments procedure

Records Management Policy
Freedom of Information Procedure
Safeguarding Policy
Behaviour Management Policy

4.0 Definitions

Data Controller
An individual or organisation that determines the purposes and means of processing personal data.
Example: York College is the data controller for staff and student information.

Designated Data Controllers
Individuals within the organisation who act on behalf of the College to ensure compliance with data protection requirements. *(Note: Legally, the College is the Data Controller; these individuals support compliance internally.)*

Data Processor
A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the data controller.

Data Subject
A living, identifiable individual to whom the personal data relates.

Data Protection Impact Assessment (DPIA)
A process designed to systematically analyse, identify, and minimise data protection risks in a project or plan.

Information Security Breach
Any security incident that compromises the confidentiality, integrity, or availability of College data.

Data Protection Legislation
Includes:
i) The UK General Data Protection Regulation (UK GDPR);
ii) The Data Protection Act 2018;
iii) The Law Enforcement Directive; and
iv) All applicable laws relating to the processing of personal data and privacy.

Facial Recognition Data
Biometric data derived from facial features used to uniquely identify an individual.
This data is collected only by cameras at the main atrium entrance, staff entrance, and construction entrance. Other CCTV cameras do not collect biometric data.

Information Commissioner's Office (ICO)
The UK's independent regulator (Supervisory Authority) appointed by Parliament to monitor compliance with data protection legislation. The ICO provides advice, investigates complaints, and takes enforcement action against organisations and individuals who fail to comply.

Personal Data
Any information relating to an identifiable living person. Identification may be direct (e.g., a

unique name, identification number) or indirect when combined with other information (e.g., name plus date of birth or address).
For further guidance, refer to the ICO: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-information-a-guide/

Processing
Any operation or set of operations performed on personal data, whether automated or not, such as collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, dissemination, alignment, restriction, erasure, or destruction.

Special Category Data
(Previously known as sensitive data) Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (e.g., fingerprints, eye scans) for identification purposes, health data, or data concerning a person's sex life or sexual orientation.

Criminal Records Data
Information about an individual's criminal convictions and offences, and related allegations or proceedings.

5.0 Roles, Responsibilities & Accountability

5.1 College Governors

Are ultimately responsible for ensuring the College complies with data protection legislation. To this end, the Governors set the policy for employees to follow that ensures this compliance.

5.2 Information Asset Owners

Senior staff members hold delegated responsibility for their areas and to understand how those areas use personal information; for example: what information is held; where it comes from; what it is used for; who it is shared with; how long it is kept, and who has access and why. They are responsible for making routine decisions about how their areas comply with data protection legislation.

The information asset owners will deal with day-to-day matters. The College has two members of staff who are designated data controllers. They are the Deputy Principal & CEO (Curriculum & Quality - for issues relating to quality and curriculum activities and information systems) and the Chief Operating Officer for issues relating to finance, audit, IT and estates within the remit of the role).

5.3 Data Protection Officer (DPO)

Responsible for providing advice and guidance to the College as to how to comply with data protection legislation. Also responsible for highlighting areas of non-compliance and risk. Acts as a single point of contact for both the ICO and individuals who want to find out about their data (see section on subject access below). The College is required to designate a DPO by law.

5.4 Staff (including consultants and contractors)

Responsible for being aware of the requirements of this policy and complying with those requirements. They are also responsible for discovering and notifying the College of Information Security Breaches, Subject Access Requests, and other subject rights requests. In addition to these responsibilities, staff are also required to maintain confidentiality as per the relevant clauses in their employment contracts.

Staff who are processing personal data on behalf of the College are required:

- to only access data that they have authority to access and only for authorised purposes.
- not to disclose data except to individuals (whether inside or outside the College) who have appropriate authorisation.
- to keep data secure (for example by complying with rules on access to premises, computer access, password protection, and secure file storage and destruction).
- not to remove personal data, or devices containing or that can be used to access personal data, from the College's premises without adopting appropriate security measures (such as encryption and password protection) to secure the data and the device; and
- not to use personal email addresses to conduct College business.
- promptly inform the data protection officer of any errors or breaches to information security.

The College cannot be held responsible for any errors unless the staff member has informed the College of them.

Compliance with GDPR is the responsibility of everyone. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken or access to college facilities being withdrawn, or even criminal prosecution.

The procedures and forms noted within this policy are available to staff via the Data Protection Hub accessed via the sharepoint site.

5.5 Students

Students should ensure that all personal data provided to the College is accurate and up to date. They should ensure that the College is notified of any changes of address, or any other personal details that are required to be provided to the College.

Students who use the College computer facilities to process personal data must comply with Data Protection legislation and the requirements set out in the College's IT Data Security Policy. Any student who requires further clarification about this should contact their tutor or IT Helpdesk personnel.

6.0 The Data Protection Principles

The six main principles of data protection are that personal data should be:

- Processed lawfully, fairly and in a transparent way
- Collected for a specific purpose
- Adequate, relevant and limited to what's necessary

- Kept up to date
- Kept for only as long as necessary
- Protected with appropriate security

A seventh general principle is that any data controller should be responsible for, and able to demonstrate, compliance with the six other principles.

7.0 Lawful Basis For processing (Data Asset Register)

To be able to process personal data lawfully, the College must ensure that all processing falls within one or more of the lawful bases (conditions for processing). These are:

- Consent – An individual has provided clear consent for the processing of their personal data for one or more specified purposes;
- Contract – The processing of the personal data is necessary to fulfil a contract that the College has with an individual;
- Legal Obligation – Processing of data is necessary to comply with the law, other than to fulfil a contractual reason;
- Vital Interests – Processing of data is necessary to protect someone's life;
- Public Task – Processing is necessary for the College to perform a public interest task or to fulfil its official functions, where the task or function has a clear legal basis;
- Legitimate Interests – Processing is necessary for the College's legitimate interests or the legitimate interests of a third party, unless the need to protect an individual's personal data overrides those legitimate interests. At each point that the College collects data, the lawful basis for processing will be made clear.

The processing of biometric data, such as facial recognition, will be based on legitimate interests and public task, as it is necessary for vandalism prevention and maintaining a safe environment. The College ensures that the processing aligns with the Data Protection Act 2018 and GDPR requirements, including conducting a balancing test to ensure that the legitimate interests do not override the rights and freedoms of individuals.

8.0 Transparency and Privacy Notices

Article 5 of the GDPR requires data controllers to be transparent about their processing of personal data. Transparency is achieved by telling subjects about this processing, and Article 13 of the GDPR sets out what information data controllers must provide to data subjects when they collect their personal data. The form in which this information is given is generally called a privacy notice, and a notice must be provided at the time the data is obtained. Signage and privacy notices are in place to inform individuals of CCTV coverage that incorporates facial recognition technology. Facial recognition cameras are installed only at the main atrium entrance, staff entrance and construction entrance.

9.0 Data Security

The following general principles apply at all times to all data managed by the College, whether the data are personal and/or special category data; confidential business data; or commercially sensitive data:

- All college users of data must ensure that all data, and specifically personal and special category data, they hold is kept securely;
- Users must ensure data is not disclosed to any unauthorised third party in any form either accidentally or otherwise (including verbal disclosure);
- Desks should be left clear at the end of each working day; paperwork shall be locked away when not in use;
- Portable devices (laptops, memory sticks, external hard drives) should not be left unattended.
- Information security incidents and breaches are reported in line with the College's IT & Data Security Policy and Data Breach Policy.

The College will implement appropriate technical and organisational measures to ensure the security of information it processes.

The College takes the security of personal data seriously. The College has internal policies and controls in place to protect personal data at rest or in transit against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by staff in the proper performance of their duties.

Biometric data is encrypted and stored securely, with access restricted to authorised personnel only. The College has implemented strict retention policies to ensure that biometric data is retained for the minimum necessary period and securely deleted when no longer needed. Regular reviews and updates to security measures are conducted to maintain data protection.

Where the College engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, ie a data sharing agreement and/or under contractual agreement. Third party suppliers are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

10.0 Information Security Breaches

All breaches of data protection should be reported to the Data Protection Officer using the breach reporting process. An assessment will be made as to whether there are significant risks to the rights and freedoms of individuals and whether a notification must be made to the Information Commissioner's Office. Any such notification must be approved by the Data Protection Officer and reported within 72 hours of the notification of the breach. Reference should be made to the College's Data Breach Policy.

Information security breaches must be reported **immediately** using the Data Breach Report Form or by email to the Data Protection Officer at dataprotection@yorkcollege.ac.uk or in their absence the Assistant Director of IT Systems & Services - ITHelpdesk@yorkcollege.ac.uk

It is essential that staff report a breach or potential breach immediately. This allows quick action to be taken to address the breach, as well as allowing the College to comply with its obligation to report breaches.

If there has been clear negligence or intent with regard to any breach of the data protection policy by members of staff or students, the College will consider the circumstances and decide how best to handle the next steps. Where a staff member has been negligent without mitigation, this will be dealt with in accordance with the College's disciplinary procedures. All factors will be taken into account when determining appropriate action, including whether the beach was reported promptly.

If the breach is likely to result in a high risk of adversely affecting the rights and freedoms of individuals, the College will inform the affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures taken.

11.0 Record of Processing Activities (Asset Register)

The College will comply with Article 30 of the GDPR by maintaining a record of its processing activities. This record will include:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries (i.e. any country outside of the European Economic Area or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data; and,

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

(h) The College will conduct an annual audit of its processing activities and update the processing record accordingly.

12.0 Processing Special Category Data

The Data Protection Act 2018 outlines safeguards for the processing of sensitive special category data. Sensitive processing is defined in s.35 (8) as;

- The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership,
- The processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual,
- The processing of data concerning health
- The processing of data concerning an individual's sex life or sexual orientation. When processing special category data the College will ensure it has identified it's lawful basis for processing as set out in Articles 9(2) and 10 of the GDPR including:
- for employment, social security and social protection purposes.
- for substantial public interest purposes.
- for archiving, research or statistics purposes

The College processes biometric data only through facial recognition cameras located at designated entrances. This processing supports the College's safety, security and vandalism prevention objectives.

The College will process special category data confidentially and only where necessary.

13.0 Individual's Rights and Subject Access Requests

13.1 The law gives data subjects specific rights over their information. These rights are:

- to be informed of our use of information about them (see Transparency & privacy notices above);
- to access information about themselves (see Subject access below);
- to rectify information about them that is inaccurate;
- to have their information erased (the 'right to be forgotten');
- to restrict how we use information about them;
- to move their information to a new service provider;
- to object to how we use information about them;
- not to have decisions made about them on the basis of automated decision making;
- to object to direct marketing; and,
- to complain about anything the College does with their information (please see Complaints section below)
- To enforce your rights through judicial remedy (i.e. by making a claim through the courts).

Some of the rights listed above apply only in certain situations, and some have a limited effect.

You can exercise any of these rights (or request more information) by emailing the College at: dataprotection@yorkcollege.ac.uk.

13.2 Subject Access Requests

Data subjects about whom the College processes information (including staff, students, and other users of the College) have the right to request access to any personal data that is being processed that relates to them either on computer or in certain files. The law entitles subjects to make requests verbally, but the College encourages subjects to put their requests in writing to maintain a record and avoid misunderstandings.

Due to the nature of CCTV footage, it is generally not practical to send copies electronically. Instead, individuals will be invited to view the footage securely at the College premises. Exceptions apply where disclosure would adversely affect the rights and freedoms of others

Subject Access requests from individuals should be made by email where possible, addressed to the Data Protection Officer at dataprotection@yorkcollege.ac.uk.

14.0 Subject Consent

It is a condition of the registration of students, and of the employment of staff, that individuals agree to York College's processing of specified classes of personal data, including special category data. The College relies on a variety of legal grounds to process information (see section on lawful basis for processing), this includes information required under contract, information which is collected under public task, and information which the College believes it has legitimate interest in processing. In some cases, the College needs to process information that, by the definition set out in the GDPR, is classed as special category data. Such information may be needed, for example, to ensure safety, to comply with the requirements of the government or of funding bodies, to provide support for staff or students or to implement institutional policies. In some of these cases, the College may need to seek specific consent from the individual.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use the College facilities do not pose a threat or danger to other users.

The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual but will need consent to process in the event of a medical emergency, for example.

15.0 Information Sharing

15.1 There are a number of situations in which personal information might be shared outside of the College, but these situations can be broken into two broad groups:

- Sharing with a data processor, who processes the information only on behalf of the College, or

- Sharing with a third party (e.g., a data controller, who processes the information for their purposes)

Personal information will only be shared in accordance with data protection legislation. If you are unsure whether sharing personal information is lawful you should seek advice from the data protection officer. More information can be found in the College's Privacy Policy on the website.

15.2 Sharing with a data processor

Personal information will only be shared with a data processor if a contract that satisfies the requirements of Article 28 of the GDPR is in place between the College and the processor.

15.3 Sharing with the police and other third parties

Specific procedures apply to the provision of data to third parties.

Personal data requests will occasionally be received from the police; requests must be made in writing and must be referred to the Data Protection Officer (dataprotection@yorkcollege.ac.uk) for approval. The exemption given to the police to pursue their enforcement functions does not cover the disclosure of all personal information held on an individual. It only allows the College to release personal information for the stated purpose(s) and only if not releasing it would be likely to prejudice legitimate investigations.

If a subject data request is received from an individual after a personal data request has been made by the police, the relevant police force must be consulted before any decision is made to release details of the personal data request to the individual.

In addition, staff must ensure the following in relation to sharing any personal data with a third party:

- when bulk sharing personal data with another organisation, advice is routinely sought from the Data Protection Officer and a Data Sharing Agreement (or other such contractual arrangement) is in place.
- where personal or sensitive information is being collected for a new operational purpose, the Data Protection Officer should always be informed.
- ensure that all requests for disclosures for personal or sensitive information are sent to the Data Protection Officer in the first instance.

Personal information can be shared with a third party under a number of scenarios, including:

- Sharing with another data controller because of a legal obligation (such as sharing staff pay details with HMRC);
- Relying on an exemption from the GDPR contained in the Data Protection Act 2018 (such as sharing with the police for the prevention and detection of crime);
- Because we are required by law to do so (sharing some student information with the Department for Education, for example); or,

- Because a subject asks us to (for example, to provide a reference to a new employer.)

Frequent and voluminous sharing should be completed under an information sharing agreement. An example of an agreement is available via the Data Protection Hub (intranet site) for managers to adapt accordingly.

Ad hoc sharing decisions should be recorded by information asset owners (see section above), including what was shared, who with, when and what considerations were made at the time.

16.0 Direct Marketing

The College is subject to certain rules and privacy laws when marketing to applicants, students, alumni and any other potential user of college services. For example, a data subject's prior Consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers (e.g. current students) known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar services (e.g. a post-graduate course or a professional qualification), and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information. A data subject's objection to direct marketing must be promptly honoured. If a data subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

17.0 International transfers

In accordance with Articles 44-49 of the GDPR, personal information will only be shared outside of the EEA where the law allows. The College will not transfer data outside of the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

The College will maintain a record of transfers of personal data to third countries. Records will be held by information asset owners (see section above).

18.0 Publication of College Information

Information that is already in the public domain is exempt from GDPR. It is College policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names and contacts of college governors

- List of key staff and roles

Any individual who has good reason for wishing further details in these lists or categories to remain confidential should contact the Data Protection Officer.

19.0 Retention of Data

In general information about students will be retained securely for 6 years from the financial year end after the end of a student's course. Some information, however, will be kept for much longer to adhere to the funding agencies requirements or awarding body regulations. This will include:

- name, address and other non-sensitive data
- academic achievements
- copies of any reference written
- other matters relating to the student's time at college

In general, all information about staff will be kept for 6 years after a member of staff leaves the College. Some information, however, will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding employment, Occupational Health records, and information required for job references. Further information is available from the Human Resources Department.

20.0 Privacy by design

The College will (in accordance with Article 25 of the GDPR) ensure that privacy and compliance with the data protection principles is considered from the earliest stages of any processing of personal data.

As Recital 78 of the GDPR describes, the College will take data protection into consideration when developing, designing and selecting systems and applications. The College will also encourage producers and suppliers of such systems and applications to account for data protection and privacy within their products.

21.0 Data protection impact assessments (DPIAs)

To comply with Article 35 of the GDPR, and to encourage the implementation of the data protection by design and default approach, the College will conduct DPIAs prior to processing any personal data where the processing presents a high risk to the rights and freedoms of data subjects.

DPIAs will be reviewed and authorised by the information asset owner and data protection officer for low residual risk processing. Medium residual risk processing will require the asset owner, DPO and Deputy Principal (Curriculum & Quality).

High residual risk processing will, in addition to the above, also require consultation with the ICO prior to the processing commencing.

More information of DPIAs, and guidance on how to carry one out, can be found within the College's Data Protection Hub, accessible by staff only.

22.0 Complaints

The College recommends that complaints about the processing of personal data by the College are addressed to the Data Protection Officer at dataprotection@yorkcollege.ac.uk in the first instance so that they can be dealt with quickly and efficiently.

Alternatively (or if you are unhappy with the way the College has handled your complaint) you may contact the Information Commissioner's Office:

Website: www.ico.org.uk
Phone: 0303 123 1113

Complaints in respect of how the College's Data Protection Officer has handled your enquiry or request should be addressed to the Principal and Chief Executive at the College.

23.0 Registration

The College is registered with the Information Commissioner's Office as a 'data controller',
registration number Z6455437. The College is listed as a public authority in Schedule 1 of the Freedom of Information Act 2000 and therefore is defined as a public authority in the UK GDPR and DPA 2018. Breaching the UK's privacy laws can result in enforcement action, including monetary penalties.

24.0 Key Contacts

For any enquiries or issues regarding the interpretation or implementation of this policy, please address them with one of the designated data controllers or the data protection officer.

Designated Data Controllers:

Deputy Principal/CEO

Chief Operating Officer

Data Protection Officer: Director of MIS & IT